**Department of Electronics & Communication Engineering**Computer Communication Networks Laboratory

Worksheet-4

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** | | | |
| **Semester:** 5 | **Section:** | **SRN:** | **Date:** |

**Lab 4: Analyse the DNS query and response using Wireshark**

1. Draw the DNS message format.

2. Run the ‘ipconfig /all’ command. It lists the different network interfaces available on your computer along with their parameters. Determine the correct network interface you are connected to and note down the following values:

|  |  |
| --- | --- |
| **Host IP Address** |  |
| **Subnet Mask** |  |
| **Local DNS Server IP Address** |  |
| **DHCP Server IP Address** |  |
| **Physical Address** |  |

(The concepts of IP addresses, physical addresses and DHCP will be seen in later units)  
  
  
3. Run the ‘ipconfig /displaydns’ command. List the fields available for each entry and briefly explain their functions:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

4. List the 4 types of DNS records, their type IDs (decimal numbers as seen above in Q3) along with a description of what value they return:

|  |  |  |
| --- | --- | --- |
| **Type** | **Type ID** | **Value** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

5. Perform the experiment as per the instructions and note down the following values:  
 (Ensure www is used wherever given)

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Hostname/Domain** | **Expected Value** | **Value** |
| A | ieeexplore.ieee.org | IP Address |  |
| CNAME | www.ieee.org | Canonical hostname |  |
| NS | www.pes.edu | Name of authoritative DNS server (nameserver) |  |
| MX | mail.google.com | Mail Server alias hostname |  |

6. What transport layer protocol does DNS use? What is the standard port number for DNS? Verify whether the DNS query was sent to the same port and the DNS response was received from the same port.  
7. Since the DNS message format is same for both queries and responses, how can we identify whether a given message is a query or a response? (Hint: Analyze all the fields of the query and response in Wireshark and notice whether any field EXPLICILTLY specifies if a given message is a query or a response).

8. We see that the DNS message format has fields named ‘Answer RRs’, ‘Authority RRs’ and ‘Additional RRs’. What does RR stand for?

9. Did the DNS queries follow the iterative mechanism or the recursive mechanism? Mention which field provides this information.

10. Once a DNS entry is made into a DNS server, does it expire after a finite time, or does it remain in the server until deletion? Justify your answer. Mention which field in the DNS response helped you arrive at this conclusion.

**Additional Exercises – DNS Attacks:**

1. Explore the term ‘DNS poisoning’ and briefly describe what it means.

2. You might have heard of the terms DoS (Denial of Service) and DDoS (Distributed Denial of Service). Explore how these attacks are different from each other and how they affect the end user.

3. Why do you think DNS uses UDP and not TCP? Does this mean that DNS data is not reliable?